How to Access the Server via SSH After Changing the SSH Port?

written by sysadmin | 24 June 2025

The previous article explained how to change the SSH port. Nevertheless, after I changed the port, I could not access the server via SSH using the new port.

Problem

How to access the server via SSH after changing the SSH port?

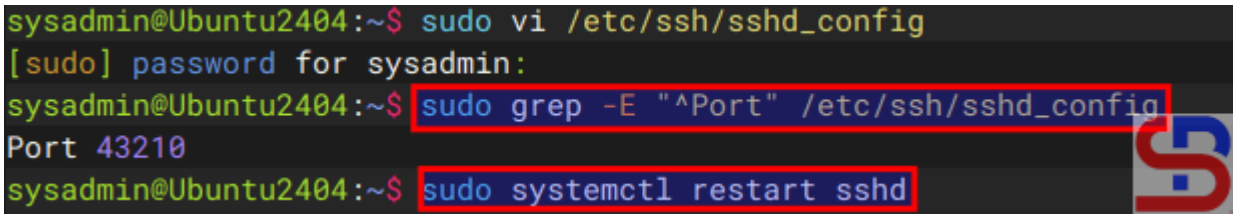
Solution

Let's say you have changed the SSH port from **port 22 to port 43210** by changing it in the **/etc/ssh/sshd_config** file and checking the port by typing the command below:

```
sudo grep -E "^Port" /etc/ssh/sshd_config
```

After that, restart the SSH using the command below:

```
sudo systemctl restart sshd
```



Change to the new port in SSH

However, you can't access the server via SSH using port 43210 but can still access via SSH port 22 as shown in the image below:

```
sysadmin@lubuntu:~$ ssh sysadmin@192.168.56.102 -p 43210
ssh: connect to host 192.168.56.102 port 43210: Connection refused
sysadmin@lubuntu:~$
sysadmin@lubuntu:~$ ssh sysadmin@192.168.56.102
sysadmin@192.168.56.102's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-60-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Sat May 17 07:07:05 2025 from 192.168.56.1
sysadmin@Ubuntu2404:~$
```

Test the result

In the remote, type the command below to check if the SSH port has changed to Port 43210 or not:

```
sudo ss -tulnp | grep sshd
```

If you find the result as shown in the image below:

```
sysadmin@Ubuntu2404:~$ sudo grep -E "^Port" /etc/ssh/sshd_config
Port 43210
sysadmin@Ubuntu2404:~$
sysadmin@Ubuntu2404:~$ sudo ss -tulnp | grep sshd
tcp   LISTEN 0      4096                 *:22               *:*    users:(("sshd",pid=1003,fd=3),("systemd",pid=1,fd=88
sysadmin@Ubuntu2404:~$
```

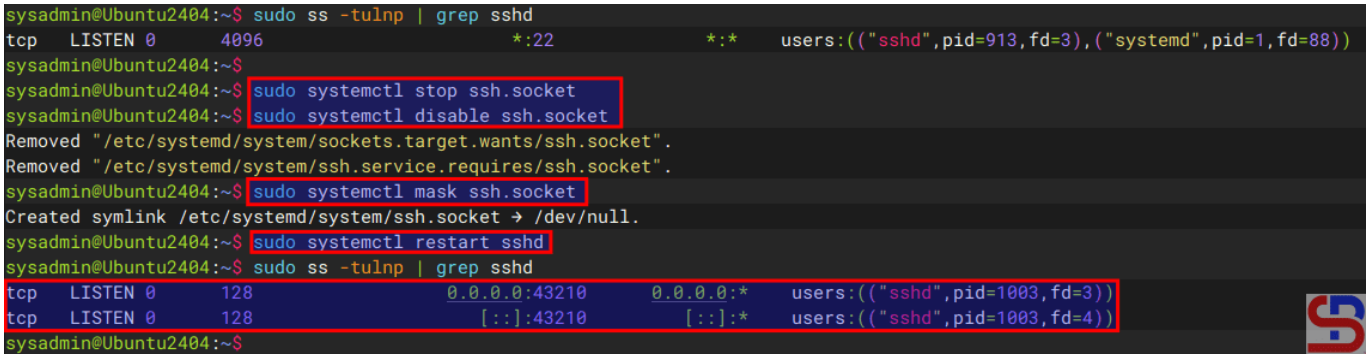
Check the port

It means the SSH is still connected to port 22 and not to port 43210. Therefore, type the commands below:

```
sudo systemctl stop ssh.socket
sudo systemctl disable ssh.socket
sudo systemctl mask ssh.socket
sudo systemctl restart sshd
```

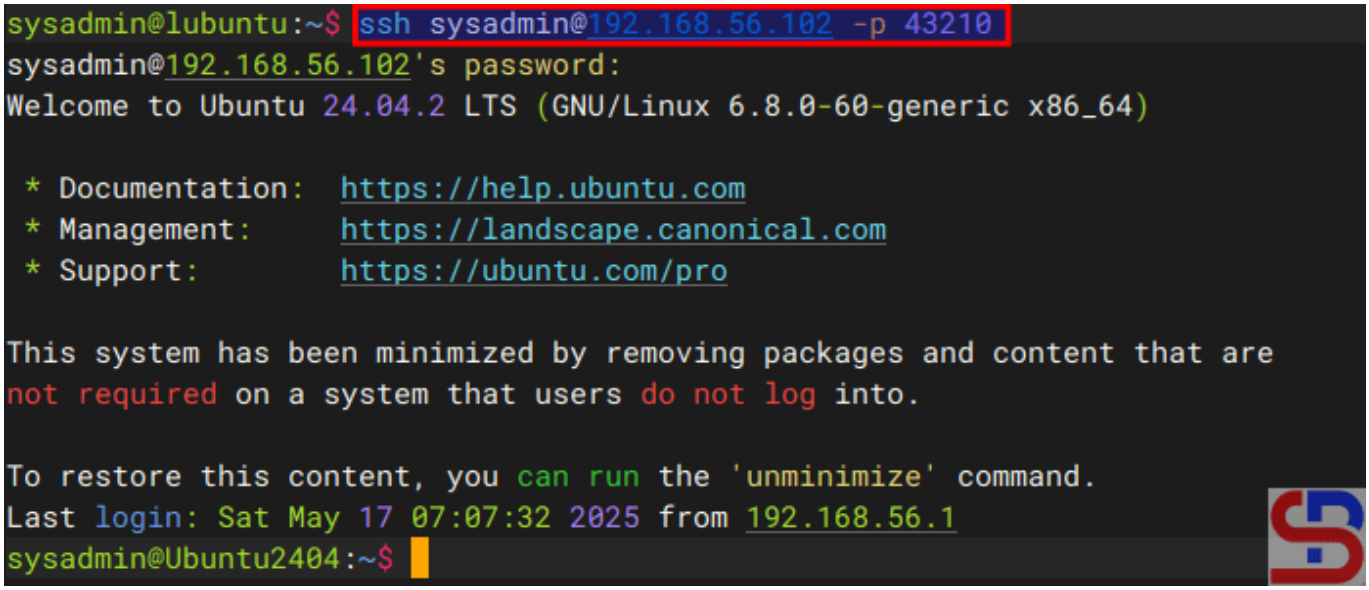
Run the previous command to check the port:

```
sudo ss -tulnp | grep sshd
```



Check the port

You can see in the image above that the SSH port has changed to port 43210 and you should be able to access the server via SSH using port 43210.



Test the result

Note

The socket statistics, or **ss**, is a tool to display network socket information. This tool has the same function as netstat but has several advantages such as faster, filtering by connection state (e.g., established, time-wait), debugging high-performance networks, and so on.

References

[askubuntu.com]

rome-rohani.medium.com
discourse.ubuntu.com
community.clearlinux.org
redhat.com